

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-307544

(43) 公開日 平成9年(1997)11月28日

(51) Int.Cl. <sup>4</sup>	識別記号	序内整理番号	F I	技術表示箇所
H 0 4 L 9/10			H 0 4 L 9/00	6 2 1 A
G 0 6 K 19/10		7259-5 J	G 0 9 C 1/00	6 4 0 D
G 0 9 C 1/00	6 4 0	7259-5 J		6 4 0 B
			G 0 6 K 19/00	R
H 0 4 L 9/32			H 0 4 L 9/00	6 7 5 B
			審査請求 未請求 請求項の数4 O L (全 7 頁)	

(21) 出願番号 特願平8-122071

(22) 出願日 平成8年(1996)5月16日

(71) 出願人 000004226

日本電信電話株式会社  
東京都新宿区西新宿三丁目19番2号

(72) 発明者 村田 祐一

東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

(72) 発明者 林 誠一郎

東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

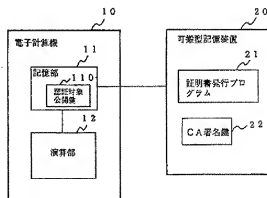
(74) 代理人 弁理士 鈴木 誠

(54) 【発明の名称】 可搬型暗号認証システム

(57) 【要約】

【課題】 証明書発行機能か不正使用されない高セキュリティを実現しつつ、認証対象者の電子計算機での証明書発行を可能にする。

【解決手段】 証明書発行プログラム21と証明書発行権者(CA)の署名鍵22を可搬型記憶装置20に格納し、該記憶装置20を電子計算機10と切り離してCAに保持せしめる。証明書発行時、CAは記憶装置20を電子計算機10に接続し、証明書発行プログラム21とCA署名鍵22を電子計算機10に転送する。電子計算機10は、該証明書発行プログラムにより、CA署名鍵を用いて、認証対象公開鍵110に対するCAの証明書を生成する。なお、電子計算機10と可搬型記憶装置20の構成の一部又は全部を可搬型電子計算機としてもよい。



## 【特許請求の範囲】

【請求項1】 可搬型の記憶装置と該可搬型記憶装置を接続可能な電子計算機とで構成される可搬型暗号鍵認証システムにおいて、

前記可搬型記憶装置は証明書発行プログラムと証明書発行権者（C A）が証明書を発行する際に用いるC A署名鍵を保持し、前記電子計算機の記憶部は認証対象者の公開鍵を保持し、

証明書発行時に、前記可搬型記憶装置を前記電子計算機に接続して、前記証明書発行プログラムとC A署名鍵を前記電子計算機の記憶部に転送し、前記電子計算機の記憶部に保有する認証対象者の公開鍵に対して、電子計算機の演算部により証明書発行処理を行うことを特徴とする可搬型暗号鍵認証システム。

【請求項2】 前記可搬型記憶装置は、証明書発行プログラムとC A署名鍵に加えて、暗号鍵生成プログラムを保持し、

証明書発行時に、前記電子計算機の演算部では、認証対象者の公開鍵を生成し、該生成した公開鍵に対して証明書発行処理を行うことを特徴とする請求項1記載の可搬型暗号鍵認証システム。

【請求項3】 記憶部と演算部を持つ可搬型の第1の電子計算機と、該第1の電子計算機に接続可能な第2の電子計算機とで構成される可搬型暗号鍵認証システムにおいて、

前記第1の電子計算機の記憶部は、証明書発行プログラムとC A署名鍵を保持し、前記第2の電子計算機の記憶部は、認証者の公開鍵を保持し、

証明書発行時に、前記第1の電子計算機を前記第2の電子計算機に接続して、前記第2の電子計算機の記憶部から認証対象者の公開鍵を前記第1の電子計算機の記憶部に転送し、前記第1の電子計算機の記憶部に保有する証明書発行プログラムとC A署名鍵を用いて、該第1の電子計算機の演算部で認証対象者の公開鍵に対する証明書発行処理を行い、該発行した証明書を第2の電子計算機の記憶部へ転送することを特徴とする可搬型暗号鍵認証システム。

【請求項4】 前記第1の電子計算機の記憶部は、証明書発行プログラムとC A署名鍵に加えて、暗号鍵生成プログラムを保有し、

証明書発行時に、前記第1の電子計算機の演算部が暗号鍵生成処理を行い、生成した公開鍵に対して、証明書発行処理を行うことを特徴とする請求項3記載の可搬型暗号鍵認証システム。

【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、情報セキュリティ技術の暗号認証機能を公開鍵暗号方式を利用して実現する場合に、可搬型の記憶装置や電子計算機を使用して公開鍵を認証するシステムに関するものである。

## 【0002】

【従来の技術】従来、公開鍵暗号方式を用いて暗号認証機能を実現する際には、認証センター（＝証明書発行権者、Certification Authority：C A）を設置し、認証対象者の公開鍵に対してC Aから発行される証明書によって公開鍵の正当性を保証するという方式がとられていた。証明書とは具体的には、公開鍵の署名対象情報としてC Aの署名鍵を用いて生成されるデジタル署名である。

【0003】また、C Aが、鍵を生成する機能を持ち、鍵生成と証明書発行の両方を行う場合もある。

## 【0004】

【発明が解決しようとする課題】従来技術においては、C Aが保持する証明書発行プログラムが第三者に不正使用されないように厳密にセキュリティ対策を講じる必要があった。また、C Aの証明書を発行してもらうために、各認証対象者は自分の公開鍵をオンラインもしくはオフラインでC Aに提出しなければならなかった。

【0005】本発明の目的は、C A機能が不正使用されないように高いセキュリティを実現しながら、認証対象者の電子計算機において証明書発行を可能にするような可搬型暗号鍵認証システムを提供することにある。

## 【0006】

【課題を解決するための手段】請求項1の発明では、証明書発行プログラムとC A署名鍵を可搬型記憶装置に格納し、該可搬型記憶装置は、認証対象者の公開鍵を保持する電子計算機と切り離してC Aが保持する。これにより、証明書発行プログラムとC A署名鍵の不正使用を防ぐと同時に、認証対象者の電子計算機に該可搬型記憶装置を接続することにより、認証対象者の電子計算機上で証明書発行処理が行えるようになる。したがって、認証対象者が自分の公開鍵をC Aに提供する必要がなくなる。

【0007】また、請求項2の発明では、暗号鍵生成プログラムも可搬型記憶装置上に保有し、認証対象者の暗号鍵生成もC Aが行うことを要旨とする。

【0008】請求項3の発明では、証明書発行プログラムとC A署名鍵を可搬型の第1の電子計算機の記憶部に格納する。この可搬型の第1の電子計算機を、認証対象者の公開鍵を保持する第2の電子計算機と切り離してC Aが保持することにより、証明書発行プログラムとC A署名鍵の不正使用を防ぐと同時に、第2の電子計算機に第1の電子計算機を接続のうえ、該第1の電子計算機の演算部で証明書発行処理が行えるようになるため、認証対象者が自分の公開鍵をC Aに提供する必要がないに加え、証明書発行プログラムとC A署名鍵が第1の電子計算機の外部に出ることがないため、さらに安全に証明書発行処理が行える。

【0009】また、請求項4の発明では、暗号鍵生成プログラムも可搬型の第1の電子計算機の記憶部に保有

し、認証対象者の暗号鍵生成も該第1の電子計算機の演算部で行うことを要旨とする。

【0010】

【発明の実施の形態】以下、本発明の各実施例について図面により説明する。

【0011】〈実施例1〉図1は本発明の第1の実施例の構成図で、10は電子計算機、20は可搬型記憶装置である。なお、可搬型記憶装置20の例としては、P C M C I A インタフェースを有するP C カード、I C メモリカード、フロッピーディスク等が考えられる。可搬型記憶装置21は、その内部に証明書発行プログラム21とC A が証明書発行するために用いるC A 署名鍵22とを保有し、電子計算機10とは独立してC A が保持しておく。電子計算機10は記憶部11と演算部12からなり、認証対象者は、証明書発行してもらいたい認証対象公開鍵110を記憶部11に保持する。

【0012】証明書発行時、C A は可搬型記憶装置20を電子計算機10に接続し、証明書発行プログラム21とC A 署名鍵22を電子計算機10の記憶部11に転送する。電子計算機10の演算部12は、この証明書発行プログラム21を用いて証明書発行処理を行う。

【0013】図2は、電子計算機10の演算部12における証明書発行処理の概要を示したものである。すなわち、記憶部11に格納された認証対象公開鍵110を証明書発行情報として証明書発行プログラムに与え、C A 署名鍵を用いて、認証対象公開鍵110に対するC A の証明書を生成する。該生成した証明書は記憶部11へ格納する。

【0014】〈実施例2〉図3は本発明の第2の実施例の構成図である。これは、図1の第1の実施例の可搬型記憶装置20の内部に保持しておくものとして、暗号鍵生成プログラム23を追加したものである。可搬型記憶装置20は電子計算機10とは独立してC A が保持しておく。

【0015】証明書発行時、C A は可搬型記憶装置20を電子計算機10に接続し、証明書発行プログラム21、C A 署名鍵22、および暗号鍵生成プログラム23を電子計算機10の記憶部11に転送する。

【0016】電子計算機10の演算部12においては、まず、暗号鍵生成プログラムを動作させ、認証対象者の暗号鍵を生成する。生成した暗号鍵は記憶部11に保持する。続いて演算部12において、図2で示す証明書発行処理を行う。すなわち、記憶部11で保持された暗号鍵のうち、認証対象公開鍵を証明書発行情報として証明書発行プログラムへ入力として与え、C A 署名鍵を用いて、認証対象公開鍵に対するC A の証明書を生成する。生成した証明書は記憶部11へ格納する。

【0017】〈実施例3〉図4は、本発明の第3の実施例の構成図で、10は第2の電子計算機B、30は第1の可搬型電子計算機Aを示すものである。なお、可搬型

電子計算機A30の例としては、CPUを持つI C カードが考えられる。該可搬型電子計算機A30の記憶部31に、証明書発行プログラム311とC A 署名鍵312を保持する。該可搬型電子計算機A30は電子計算機B10とは独立してC A が保持しておく。電子計算機B10の構成は図1の実施例と同様である。

【0018】証明書発行時、C A は可搬型電子計算機A30を電子計算機B10に接続する。認証対象者は、電子計算機B10の記憶部11内の証明書発行してもらいたい認証対象公開鍵110を可搬型電子計算機A230記憶部31へ転送する。そして、該可搬型電子計算機A30の演算部32において、図2で示す証明書発行処理を行う。すなわち、記憶部31に転送された認証対象公開鍵を証明書発行情報として証明書発行プログラム311に入力として与え、C A 署名鍵312を用いて、認証対象公開鍵に対するC A の証明書を生成する。該生成した証明書は電子計算機B10の記憶部11へ転送する。

【0019】〈実施例4〉図5は、第4の実施例の構成図である。これは、図4の第3の実施例における第1の可搬型電子計算機A30の記憶部31に保持しておくものとして、暗号鍵生成プログラム313を追加したものである。該可搬型電子計算機A30は第2の電子計算機B10とは独立してC A が保持しておく。

【0020】証明書発行時、C A は可搬型電子計算機A30を電子計算機B10に接続する。そして、まず、該可搬型電子計算機A30の演算部32において、暗号鍵生成プログラム313を動作させ、認証対象者の暗号鍵を生成する。該生成した暗号鍵は記憶部31に保持する。続いて、該可搬型電子計算機A30の演算部32において、図2で示す証明書発行処理を行う。すなわち、記憶部31で保持された暗号鍵のうち、認証対象公開鍵を証明書発行情報として証明書発行プログラム311へ入力として与え、C A 署名鍵312を用いて、認証対象公開鍵に対するC A の証明書を生成する。最後に、生成した証明書を電子計算機B10の記憶部11へ転送する。

【0021】

【発明の効果】以上説明したように、本発明によれば、認証対象者の公開鍵に対する証明書発行機能を可搬型記憶装置もしくは可搬型電子計算機に格納し、それらをC A が管理することで不従用を防ぐことが可能になり、さらにそれらの可搬型記憶装置、もしくは可搬型電子計算機を認証対象者の電子計算機に接続して証明書発行処理が可能になるため、認証対象者が自分の公開鍵をC A に提出しなくても証明書を発行してもらうことが可能になる。

【図面の簡単な説明】

【図1】本発明の第1の実施例の構成図である。

【図2】証明書発行プログラムの動作概要を示す図であ

る。

【図3】本発明の第2の実施例の構成図である。

【図4】本発明の第3の実施例の構成図である。

【図5】本発明の第4の実施例の構成図である。

【符号の説明】

10 電子計算機

11 記憶部

110 認証対象公開鍵

12 演算部

20 可搬型記憶装置

\* 21 証明書発行プログラム

22 CA署名鍵

23 暗号鍵生成プログラム

30 可搬型電子計算機

31 記憶部

311 証明書発行プログラム

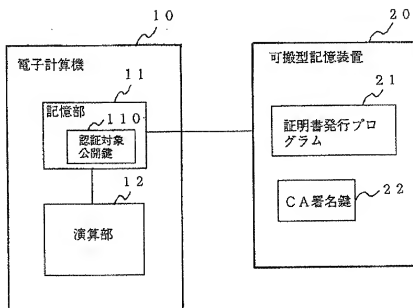
312 CA署名鍵

313 暗号鍵生成プログラム

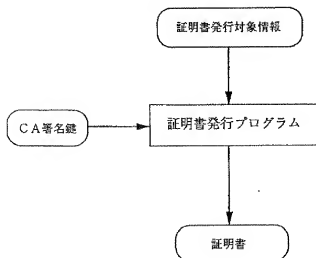
32 演算部

\*10

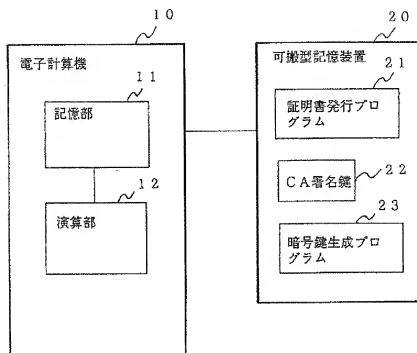
【図1】



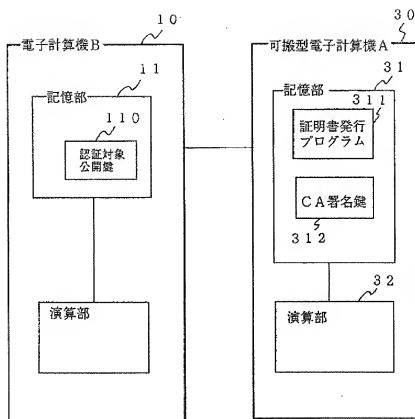
【図2】



【図3】



【図4】



【図5】

